

Claims:

What is claimed is:

1. A system for single security administration comprising:
5 a first server that includes an LDAP authentication server;
a second server that includes an embedded LDAP server;
a default security plugin at said first server that receives authentication requests from clients and forwards them to said LDAP authentication server; and,
10 wherein, in response to receiving a request for authentication from a client, the system initiates an LDAP session between said first server and said second server, passes query information from said LDAP authentication server to said embedded LDAP server, receives corresponding user information, and creates a token that reflects an authentication result that can be used by said
15 client.
2. The system of claim 1 wherein the system checks a user profile database or user profile configuration information to determine where the user security information is stored.
20
3. The system of claim 1 wherein said first server is a WebLogic server.
4. The system of claim 1 wherein said second server is a Tuxedo server.
- 25 5. The system of claim 1 wherein said first server is a WebLogic server, and said second server is a Tuxedo server.

6. The system of claim 1 wherein said client is a Tuxedo client and said request is a tpinit call.

7. The system of claim 1 wherein said query information is query user
5 information that specifies a particular user or group of users.

8. The system of claim 1 wherein the system includes a plurality of servers

9. The system of claim 8 wherein at least two of said plurality of servers
10 include an LDAP authentication server.

10. The system of claim 1, further comprising a user information cache that caches a copy of said user information.

11. The system of claim 1 wherein the system is scalable to include multiple
15 LDAP authentication servers and/or multiple embedded LDAP servers.

12. The system of claim 1 wherein at least one of said servers include a console program for administering the security of the system.

20

13. A method for providing single security administration comprising the steps of:

issuing a call to an LDAP authentication server at a first server;

passing query user information from said LDAP authentication server to

25 an embedded LDAP server at a second server;

returning corresponding user information to said LDAP authentication server; and,

providing an authentication token for use by the client.

14. The method of claim 13, further comprising the step, prior to issuing a call, of allowing a client to access a default security plugin.

5

15. The method of claim 13 wherein the system checks a user profile database or user profile configuration information to determine where the user security information is stored.

10 16. The method of claim 13 wherein said first server is a WebLogic server.

17. The method of claim 13 wherein said second server is a Tuxedo server.

15 18. The method of claim 13 wherein said first server is a WebLogic server, and said second server is a Tuxedo server.

19. The method of claim 13 wherein said client is a Tuxedo client and said request is a tpinit call.

20 20. The method of claim 13 wherein said query information is query user information that specifies a particular user or group of users.

21. The method of claim 13 wherein the system includes a plurality of servers

25 22. The method of claim 21 wherein at least two of said plurality of servers include an LDAP authentication server.

23. The method of claim 13, further comprising a user information cache that caches a copy of said user information.

24. The method of claim 13 wherein the system is scalable to include multiple
5 LDAP authentication servers and/or multiple embedded LDAP servers.

25. The method of claim 13 wherein at least one of said servers include a console program for administering the security of the system.

10 26. A system for single security administration comprising:
an application server that includes an embedded LDAP server; and,
wherein, in response to receiving a request for authentication from a client
of another enterprise server, the system initiates an LDAP session between said
application server and said other enterprise server, receives query information
15 from an LDAP authentication server at said other enterprise server, creates a
token that reflects an authentication result that can be used by said client, and
communicates said token to the other enterprise server.

20 27. The system of claim 26 wherein the system checks a user profile
database or user profile configuration information to determine where the user
security information is stored.

28. The system of claim 26 wherein said application server is a WebLogic
server.

25

29. The system of claim 26 wherein said other enterprise server is a Tuxedo
server.

30. The system of claim 26 wherein said application server is a WebLogic server, and said second other enterprise is a Tuxedo server.

5 31. The system of claim 26 wherein said client is a Tuxedo client and said request is a tpinit call.

32. The system of claim 26 wherein said query information is query user information that specifies a particular user or group of users.

10 33. The system of claim 26 wherein the system includes a plurality of servers

34. The system of claim 33 wherein at least two of said plurality of servers include an LDAP authentication server.

15 35. The system of claim 26, further comprising a user information cache that caches a copy of said user information.

36. The system of claim 26 wherein the system is scalable to include multiple LDAP authentication servers and/or multiple embedded LDAP servers.

20

37. The system of claim 26 wherein at least one of said servers include a console program for administering the security of the system.

25 38. A method for single security administration comprising:
receiving, at an LDAP server at an application server, a request for authentication from a client of another enterprise server;
initiating an LDAP session between said application server and said

other enterprise server;

receiving query information from an LDAP authentication server at said other enterprise server; and,

5 creating a token that reflects an authentication result that can be used by said client; and,

communicating said token to said other enterprise server.

39. The method of claim 38 wherein the system checks a user profile database or user profile configuration information to determine where the user security information is stored.

40. The method of claim 38 wherein said application server is a WebLogic server.

15 41. The method of claim 38 wherein said other enterprise server is a Tuxedo server.

42. The method of claim 38 wherein said application server is a WebLogic server, and said second other enterprise is a Tuxedo server.

20

43. The method of claim 38 wherein said client is a Tuxedo client and said request is a tpinit call.

25 44. The method of claim 38 wherein said query information is query user information that specifies a particular user or group of users.

45. The method of claim 38 wherein the system includes a plurality of servers

46. The method of claim 45 wherein at least two of said plurality of servers include an LDAP authentication server.

5 47. The method of claim 38, further comprising a user information cache that caches a copy of said user information.

48. The method of claim 38 wherein the system is scalable to include multiple LDAP authentication servers and/or multiple embedded LDAP servers.

10 49. The method of claim 38 wherein at least one of said servers include a console program for administering the security of the system.